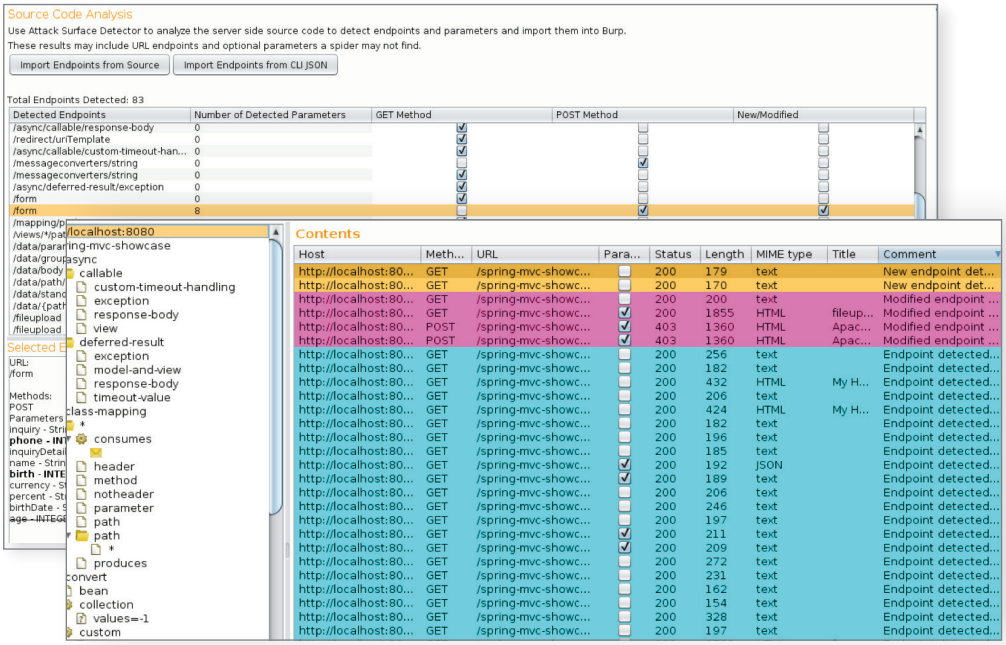
Attack Surface Detector

FACT SHEET

Uncover your hidden attack surface with the Attack Surface Detector (ASD) plugin for OWASP ZAP and Burp Suite



Automated penetration tests are a popular and effective method to identify exploitable vulnerabilities for an application, but often suffer capability gaps that are difficult to overcome with current tools. The most significant problem is that an application's attack surface is often not fully enumerated prior to testing, and consequently part of that attack surface goes unexercised. Currently, unlinked endpoints must be identified by manual code review, which is a time-consuming—and therefore expensive—process.

The Attack Surface Detector, under the ASTAM program, consists of a pair of plugins for widely adopted DAST tools, Portswigger's Burp Suite and OWASP ZAP (Zed Attack Proxy). These plugins will automatically examine the application's source code via static analysis, finding hidden or unlinked endpoints in the process, and further identifying their optional parameters and data types, which most DAST scans will miss. This greatly broadens the visible, testable portions of the application's attack surface, providing the basis for more thorough penetration testing. This newly enumerated surface can then be spidered and tested with Burp Suite or OWASP ZAP, or manually pen-tested.

About

Attack Surface Detector was developed under the DHS S&T ASTAM contract #HHSP233201600058C. It is available with the download links on the right and at: **https://github.com/secdec/**

KEY FEATURES

- Identifying of unlinked endpoints
- Uncovering optional parameters
- Uncovering parameter datatypes and names
- Leveraging attack surface difference generator to highlight differences between selected versions of your application
- Automatically generating HTTP requests based on metadata discovered during hybrid analysis
- Leveraging Burp and ZAP pen testing tools using ASD identified endpoints and parameters within a common testing environment
- Ability to import endpoints from the ASD command line interface (CLI) tool output, eliminating the need to provide direct access to source code

KEY BENEFITS

- **Identify attack surface gaps** – fills in gaps in the visible attack surface by locating unlinked endpoints that go unobserved during traditional spidering and brute force testing efforts
- **Enhanced parameter detection** – identifies optional parameters that could go unnoticed which may open back door vulnerabilities in your applications
- **Reduced effort and costs** – reduced manual efforts to detect attack surface gaps and optional parameters saves time and money
- **Focus of penetration testing** on newly identified attack surfaces
- **Easy installation** – available as an open source project through GitHub, the OWASP ZAP Marketplace and coming soon to the PortSwigger BApp Store

SUPPORTED FRAMEWORKS

Struts	Django	Ruby on Rails	ASP.NET MVC
ASP.NET Web Forms	JSP/Java Servlets	Spring MVC	

FUTURE ENDEAVORS

- PHP support is being added through community collaboration
- Process multiple frameworks for the same project
- Integration of ASD into more automated pen testing pipelines

DOWNLOAD LINKS

https://github.com/secdec/attack-surface-detector-zap

https://github.com/secdec/attack-surface-detector-burp

https://github.com/secdec/attack-surface-detector-cli

https://www.owasp.org/index.php/OWASP_Attack_Surface_Detector_Project

SECURE DECISIONS
A DIVISION OF APPLIED VISIONS, INC.

ASTAM

OWASP
Open Web Application Security Project

6 Bayview Avenue, Northport, NY 11768
(631) 759-3988 • info@securedecisions.com